

CLINICAL CONSULTATION INFORMATION SHARING METHOD

Patent Number: JP10111897
Publication date: 1998-04-28
Inventor(s): KIDO KUNIIHIKO; SANO KOICHI
Applicant(s): HITACHI LTD
Requested Patent: ☐ JP10111897
Application Number: JP19960265745 19961007
Priority Number(s):
IPC Classification: G06F19/00; G06F17/60; G06F17/30; G09C1/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To share clinical consultation data on condition that the privacy of an individual is protected and security is secured by providing a means which adds an access control setting file as one attribute of medical consultation information of a patient of each medical organ, and exchanging clinical consultation information on the patient according to the access control setting file.

SOLUTION: A hospital 101 and a hospital 102 performs a mutual authenticating process about whether or not they have the right to exchange clinical consultation data on the patient A. Then a random number R generated on the side of the hospital 101 is sent together with the ID number of the patient A according to the address HOSP of a file server 105 of the hospital 102 in the access control setting file. The file server 105 of the hospital 102 takes the mutual authentication key Ak of the access control setting file out of a clinical consultation data storage file of the patient A. Then Ak(R) generated by ciphering the random number R with the authentication key Ak and the random number R generated at the hospital 102 are sent back to the hospital 101 according to the address HOSP of a file server 104 of the hospital 101 in the access control setting file.

Data supplied from the esp@cenet database - I2

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-111897

(43)公開日 平成10年(1998) 4月28日

(51)Int.Cl. ⁶	識別記号	F I	
G 0 6 F 19/00		G 0 6 F 15/42	H
17/60		G 0 9 C 1/00	6 6 0 D
17/30		G 0 6 F 15/21	3 6 0
G 0 9 C 1/00	6 6 0	15/40	3 2 0 B
		15/42	J
審査請求 未請求 請求項の数5 O L (全 7 頁)			

(21)出願番号 特願平8-265745

(22)出願日 平成8年(1996)10月7日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 木戸 邦彦

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 佐野 耕一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 弁理士 小川 勝男

(54)【発明の名称】 診療情報共有化方法

(57)【要約】

【課題】複数医療機関にまたがり患者の診療データを共有する際に、患者のプライバシー保護と安全性を確保した上で、診療データ共有化を図ることを目的とする。

【解決手段】患者ごとに、複数の医療機関のネットワーク103上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むファイルを患者本人が任意に作成する手段と、前記ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、前記ファイルに基づき形成される各医療機関間での当該患者のための安全なアクセス経路を介して、当該患者の診療情報を安全に共有化する。

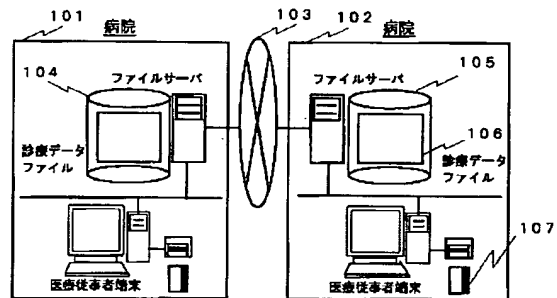


図1

【特許請求の範囲】

【請求項1】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、患者ごとに、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むアクセス制御設定ファイルを作成する手段と、前記アクセス制御設定ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記アクセス制御設定ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、前記アクセス制御設定ファイルに基づき当該患者の診療情報を安全に交換することを特徴とする診療情報共有化方法。

【請求項2】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むアクセス制御設定ファイルを、可搬媒体が有する記憶装置に記憶して管理することを特徴とする請求項1の診療情報共有化方法。

【請求項3】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、請求項1のアクセス制御設定ファイルに含まれる複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルについて、新たに追加される医療機関は、前記テーブルに含まれるネットワーク上の各アドレスに対して、当該医療機関のアドレスを送付することを特徴とする請求項1の診療情報共有化方法。

【請求項4】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報システムにおいて、患者に対する診療データの通信に際しては、請求項1のアクセス制御設定ファイルに含まれる相互認証処理に使用する鍵で相互認証し、暗号化用の鍵で暗号化して通信することを特徴とする請求項1の診療情報共有化方法。

【請求項5】複数の医療機関に分散設置された通信端末装置と、通信網により結合されて複数の医療機関によって共有される複数のデータベース、および上記通信端末装置との間で診療情報のやりとりができる広域医療情報

システムにおいて、患者は、請求項1のアクセス制御設定ファイルに患者固有の秘密鍵で電子署名したものを、前記アクセス制御設定ファイルに含まれる複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルの各アドレスに送信することを特徴とする請求項1の診療情報共有化方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、複数医療機関において、患者の診療情報を安全に共有する手段を提供するものであり、広域医療情報システムに関する。

【0002】

【従来の技術】複数医療機関をまたいで、診療情報を共有する方法として、患者のプライバシー保護の観点から、保健医療カードとよばれるICカードで行われ場合が多い。ICカードは、患者本人が携帯しており、本人がそのカードを第3者に貸したり、譲渡しない限り、カードの中身の安全性が保たれる。加えて、ICカードには、カード自体にマイクロプロセッサが埋め込まれていて、そのマイクロプロセッサで暗証番号によるアクセス権のチェックが行える。従って、ICカード内のデータは、ICカードにアクセス権限のない不特定な第3者に知られることはない。通常、このアクセス権限は、カード所有者本人や医師などに与えられるのが普通である。

【0003】

【発明が解決しようとする課題】このように、ICカードに情報を記録して、複数医療機関で診療情報を共有する方法は、強固なプライバシー保護が達成できる反面、医師の手にカードがない限り患者情報を調べることができない不便さがある。例えば、ある患者が複数の医療機関を同時に受診している場合、各医療機関で処方された薬品、最近行われた検査結果、診断内容等をその患者を受け持っている各主治医が把握することは大切であるが、患者がカードを携帯して主治医のもとに来た時以外、カード内の情報を得ることができない。従って、主治医が、患者の来院前にその患者の各種情報を前もって調べておき、今後の診断治療に役立てるなどの行為は事実上不可能である。このように、ICカードをベースとして、複数医療機関で診療情報を共有する方法では、患者に対する情報を主治医が知りたいときにタイムリーに得ることができないという問題がある。

【0004】

【課題を解決するための手段】患者ごとに、複数の医療機関のネットワーク上でのアドレス一覧が記述されたテーブルと、当該患者のために割り当てた暗号化用の鍵と、各医療機関同士の相互認証処理に使用する鍵を含むファイルを患者本人が任意に作成する手段と、前記ファイルが確かに当該患者に関するものであることを各医療機関が認証する手段と、前記ファイルを各医療機関の当該患者の診療情報の一属性として付加する手段を有し、

前記ファイルに基づき形成される各医療機関間での当該患者のための安全なアクセス経路を介して、当該患者の診療情報を安全に共有化することにより達成することができる。

【0005】

【発明の実施の形態】

「実施例1」本発明の実施の形態として、ある患者Aが2つの医療機関を受診した場合について説明する。まず、実施例1として、上記、患者A専用の安全なアクセス経路を形成するためのアクセス制御設定ファイル201を共有する手段として、ICカードを利用する場合について説明する。図1は、システム全体の構成について説明したものである。また、図2は、本実施例で使用するファイルの構成を示したものである。この図では、病院101と病院102の二つのエンティティ間での患者Aの診療データ共有を想定している。ここで、患者Aは、病院102を受診した後に、病院101を受診したとする。病院101と病院102は、病院外部のネットワーク103に公開されたファイルサーバ104、105を持つ。ファイルサーバ104、105には、病院で診察治療を受けた患者のカルテデータが登録されている。この図では、ファイルサーバ105にある患者Aの診療データ106が登録されていると想定している。患者Aは保健医療カード107を所持している。ここで、保健医療カードとは、診察カード、保険カードなど、保健医療に関するICカードなどのセキュアな媒体を意味する。

【0006】「アクセス制御設定ファイル生成と診療データファイル生成」保健医療カード107内のアクセス制御設定ファイル生成と患者Aの診療データファイル生成について説明する。

【0007】(1) 患者Aは、アクセス制御設定ファイル201の生成を保健医療カード107に指示する。この時、保健医療カード107の鍵生成モジュール302において、乱数R1を生成し、これをカード内のマスタ鍵により暗号化して鍵Dkを生成し、アクセス制御設定ファイル記憶領域301の暗号化用鍵の記憶領域303に登録する。同様に、保健医療カード107の鍵生成モジュール302は、乱数R2を生成し、これをカード内のマスタ鍵により暗号化して鍵Akを生成し、アクセス制御設定ファイル記憶領域301の相互認証用鍵の記憶領域304に登録する。(図3)

(2) 病院102は、ファイルサーバ105に患者A用の診療データファイルを作成する。そして、病院102を訪れた患者Aは、アクセス制御設定ファイル記憶領域301の医療機関のアドレステーブル305に病院102のアドレスHOSP2を登録してもらう。

【0008】(3) (2)の処理を、患者Aは病院101を訪れたときにも行う。病院101は、ファイルサーバ104に患者A用の診療データファイルを作成する。

そして、アクセス制御設定ファイル記憶領域301の医療機関のアドレステーブル112に病院101のアドレスHOSP1を登録してもらう。

【0009】ここで、上記、病院101および102のアドレスとは、ファイルサーバ104と105のネットワーク103の所在のことである。

【0010】「アクセス制御設定情報の設定」保健医療カード107内のアクセス制御設定ファイルに基づき、患者Aの診療データファイルにアクセス制御設定情報をセットする手続きについて説明する。

【0011】(1) 病院101においては、患者Aが来院したときに、アクセス制御設定ファイル201の内容を、保健医療カード107のアクセス制御設定ファイル記憶領域301から読みとれば良い。これにより、病院101は、アクセス制御設定ファイル201の暗号化用鍵、相互認証鍵、そして病院102のアドレスHOSP2を得ることが可能である。

【0012】(2) 病院102においても同様に、アクセス制御設定ファイル201の内容を、保健医療カード107のアクセス制御設定ファイル記憶領域301から読みとる。ここで、病院102では、アクセス制御設定ファイル201の暗号化用鍵、相互認証鍵に関する情報は、保健医療カード107から読み取ることが可能であるが、アドレステーブル205は空欄である。従って、病院102を受診した患者Aが、その後に受診した病院について(この実施例では病院101)のアドレスは、別手段で得る必要がある。ここでは、病院101から次の手段で病院101のアドレスを配送してもらう。病院101は、(1)で読みとったアクセス制御設定ファイル201の医療機関のアドレステーブル112をサーチする。この例の場合には、病院102のみが登録されているので、そのアドレスのみを取り出す。そして、アクセス制御設定ファイル201の相互認証用鍵で病院102と病院101の相互認証を行った後に、患者AのID番号とともに病院101のアドレスHOSP1をアクセス制御設定ファイル201の暗号化用鍵で暗号化して病院102に送る。以上により、病院102は、患者Aに対する、アクセス制御設定ファイル201の暗号化用鍵、相互認証鍵、そして病院101のアドレスHOSP1を得ることができた。ここで、上記、アクセス制御設定ファイル201の医療機関のアドレステーブル112をサーチした時点で、複数医療機関のアドレスが登録されている場合には、その病院すべてに自分のアドレス(この場合、病院101のアドレス)をマルチキャストする。

【0013】(3) (1) (2)により、病院101および病院102において得られたアクセス制御設定情報は、病院101および病院102において、ファイルサーバ104、105における患者Aの診療データファイル206(電子カルテデータ)のアクセス制御設定情報

208に取り込み診療情報の一属性として管理する。

【0014】診療データの場合、患者のプライバシー保護の観点から、安全なアクセス経路を規定する情報(上記実施例のファイル201)は、当該患者の診療データの一属性として管理する必要がある。また、アクセス制御設定ファイル201が、確かに患者Aのものであるという認証は、患者Aが各病院を訪れた際に、信頼できる第三者機関により発行された保健医療カードを患者から直に受けとり、アクセス制御設定ファイル201の情報を得ていることにより保証される。

【0015】次に、患者Aの診療情報を、病院101と病院102がネットワーク103を介して通信しあいデータ交換を図る手段について説明する。例えば、病院101が病院102の患者Aの診療データファイル106を参照するとする。次に、図4の説明をする。

【0016】(1)病院101と病院102は、患者Aの診療データ交換を行う権利があるかどうか相互認証処理を行う。ここでは、相互認証処理として3パス相手認証方法を適用する。

【0017】1)患者AのID番号とともに、病院101側で生成した乱数Rを、アクセス制御設定ファイル201の病院102のファイルサーバ105のアドレスHOSP2に基づき送信する。

【0018】2)病院102のファイルサーバ105は、患者Aの診療データ保存ファイルから、アクセス制御設定ファイル201の相互認証鍵Akを取り出す。そして、Akで乱数Rを暗号化したAk(R)と病院102で生成した乱数Sを、アクセス制御設定ファイル201の病院101のファイルサーバ104のアドレスHOSP1に基づき病院101に送り返す。

【0019】以降、病院101と病院102の通信は、アドレスHOSP1、HOSP2に基づき行うものとする。

【0020】3)病院101は、送られてきたAk(R)を、相互認証鍵Akで復号し、1)で送信した乱数Rと一致すれば、病院101は病院102が患者Aの診療データを所有していることがわかる。もし一致しなければ、以降の処理を中止し、患者Aの診療データ交換を中止する。

【0021】4)病院101は、乱数Sを相互認証用鍵Akで暗号化したAk(S)を病院102に送信する。

【0022】5)病院102は、送られてきたAk(S)を相互認証用鍵Akで復号し、2)で送信した乱数Sと比較する。一致すれば、病院102は、病院101が患者Aの診療データへのアクセス権を有することが分かる。もし一致しなければ、以降の処理を中止し、患者Aの診療データ交換を中止する。

【0023】(2)病院102のファイルサーバ105は、本セッションにおけるデータ暗号化用セッション鍵とデータ認証用セッション鍵を生成する。

【0024】1)患者Aの診療データ保存ファイルから、アクセス制御設定ファイル201の暗号化処理用鍵Dkを取り出す。

【0025】2)病院102のファイルサーバ105は、乱数T1、T2を生成し、暗号化処理用鍵Dkにより暗号化して、データ暗号化用セッション鍵DTkとデータ認証用セッション鍵MTkを生成する。

【0026】(3)(2)で生成した、データ暗号化用セッション鍵DTkとデータ認証用セッション鍵MTkを、病院102は相互認証用鍵Akで暗号化したAk(DTk)とAk(MTk)を病院101に送信する。病院101は、(3)で送られてきたAk(DTk)とAk(MTk)を復号して、データ暗号化用セッション鍵DTkとデータ認証用セッション鍵MTkを取り出す。

【0027】(4)病院102は、診療データ106に対して、所定のハッシュ関数によりメッセージダイジェストを生成し、データ認証用セッション鍵MTkで暗号化した認証コードを作成する。次に、生成した認証コードを診療データ106に付加したものを、データ暗号化用セッション鍵DTkで暗号化する。これを、病院101に送信する。

【0028】(5)病院101では、(4)で送られてきたデータについて、データ暗号化用セッション鍵DTkで復号し、診療データ106と認証コードを取り出し、診療データ106に対して、所定のハッシュ関数によりメッセージダイジェストを生成し、データ認証用セッション鍵MTkで暗号化した認証コードを送られた認証コードと比較する。一致すれば正しい患者Aの診療データである。

【0029】以上により、病院101と病院102の間で、データ認証とデータ暗号化により、患者Aに関する診療データを安全に共有化することが可能となる。ここで、上記構成をとることによる一つの特徴がある。病院101は、来院した患者Aの情報は病院102のファイルサーバから参照することは可能であるが、病院101に来院していない患者の診療データは参照不可能である。これは、患者Aの診療データ交換を行う権利があるかどうか、患者Aの相互認証用鍵で相互認証処理を行い、この処理で相互認証が成立しない限りデータ交換が行えないからである。この特徴により、患者の主治医あるいは主治医が在籍する病院以外からの診療データ参照が不可能になるため、患者のプライバシー保護が可能になる。

【0030】本発明のもう一つの特徴について説明する。まず最初に、診療データについての特徴について簡単に説明する。診療データは、ある患者の診療の過程で発生したデータを蓄積したものであるから、それを記録する主治医とともに患者自身の所有物と考えられる。すなわち、診療データには、利用者(医療従事者)とその

所有者が完全に一致しないという特徴がある。これにより、診療データの安全性確保に厄介な問題が生じる。例えば、診療データの利用者側である複数医療機関が適当なグループを組織し、そのグループ内で安全な通信路を静的に構築したとしても、診療データの所有者である患者が、このグループ内の医療機関だけを受診するとは限らない。これにより、上記、医療機関グループの一つを受診した患者が、このグループ内の他の医療機関を受診する限りにおいては、安全に診療データのやりとりが可能なのであるが、このグループ以外の医療機関を受診した場合に、この医療機関との診療データ交換の安全性は確保できなくなる。診療データの所有者である患者は、生涯でいろいろな地域の複数の医療機関を受診するのが一般的であり、患者の受診行動範囲が上記グループ内の医療機関に一致するという想定は受け入れられない。従って、上記実施例のように、患者が受診した医療機関同士で動的に患者ごとの安全なアクセス経路を設定していく仕掛けが必要である。

【0031】最後に、上記実施例では、2つの病院を対象に説明しているが、3つ以上の医療機関における診療データ共有も同様である。

【0032】「実施例2」次の実施例では、図5のように患者Aの在宅から、ネットワーク503を介して、アクセス制御設定ファイル201を病院501と病院502に配布する。この実施例では、患者Aは何らかの別手段で病院501のアドレスHOSP3と病院502のアドレスHOSP4を知っているものとする。

【0033】「アクセス制御設定ファイル生成」(図6)患者A宅において、保健医療カード107でアクセス制御設定ファイル201を生成する手続きを図6を用いて説明する。

【0034】(1)患者Aは、アクセス制御設定ファイル201の生成を保健医療カード107に指示すと。この時、保健医療カード107の鍵生成モジュール302において、乱数R1を生成し、これをカード内のマスタ鍵により暗号化して鍵Dkを生成し、アクセス制御設定ファイル記憶領域601の暗号化用鍵の記憶領域603に登録する。同様に、保健医療カード107の鍵生成モジュール602は、乱数R2を生成し、これをカード内のマスタ鍵により暗号化して鍵Akを生成し、アクセス制御設定ファイル記憶領域601の相互認証用鍵の記憶領域604に登録する。

【0035】(2)病院501のアドレスHOSP3をアクセス制御設定ファイル記憶領域601のアクセステーブルの記憶領域605に登録する。同様に、病院502のアドレスHOSP4をアクセステーブルの記憶領域605に登録する。

【0036】(3)アクセス制御設定ファイル記憶領域601に記録されたアクセス制御設定ファイル201に、保健医療カード107の秘密鍵Saで電子署名す

る。

【0037】(4)患者Aの端末507に、(3)で電子署名したアクセス制御設定ファイル201をダウンロードする。

【0038】「アクセス制御設定ファイルの配送」アクセス制御設定ファイル201を病院501、病院502に配送する手続きについて説明する。

【0039】(1)患者Aの端末507から、病院501のアドレスHOSP3と病院502のアドレスHOSP4に基づき、電子署名したアクセス制御設定ファイル201を各病院に送信する。

【0040】(2)各病院では、送信されたアクセス制御設定ファイル201について、保健医療カード107の秘密鍵Saに対応する公開鍵Paで電子署名を検証した後、病院501と病院502は、アクセス制御設定ファイル201を患者Aの診療データファイルに登録する。

【0041】ここで、公開鍵Paが確かに患者Aのものであることは、信頼できる第三者機関が公開鍵証明書を発行していることにより保証されているものとする。

【0042】以上により、病院501と病院502において、患者Aのアクセス制御設定ファイルが得られたので、以降、診療データの共有は、実施例1と同じである。また、この例では、二つの病院を例に説明したが、三つ以上の医療機関においても同様である。

【0043】

【発明の効果】各患者ごとの、アクセス制御設定ファイル201を各医療機関で共有し、それを当該患者の診療情報データの一属性として管理することで、まず、アクセス制御設定ファイル201の医療機関のアドレステーブル205により複数医療機関にまたがる当該患者の診療データ同士がネットワーク上でリンクされる。しかも、アクセス制御設定ファイル201で管理する暗号化用鍵と相互認証用鍵により、当該患者の診療データ同士がネットワーク上でのリンクは、データの完全性と機密性が確保できる。また、相互認証用鍵を利用した相互認証処理により、患者の主治医または受診した病院以外の、医療従事者からのアクセスが禁止されることにより、患者のプライバシーが確保できる。以上、患者の診療データ同士がネットワーク上で安全にリンクされるので、患者の主治医または受診した病院からは、常時、当該患者のデータを安全に共有することが可能になる。

【図面の簡単な説明】

【図1】本発明の実施例のシステム構成図

【図2】本発明の実施例において使用するファイルの構成図

【図3】本発明の実施例における保健医療カード内での処理を表わす図

【図4】本発明の実施例における診療データ共有のためのプロトコルを示す図

【図5】本発明の実施例のシステム構成図

【図6】本発明の実施例における保健医療カード内での処理を表わす図

【符号の説明】

101…病院、102…病院、103…ネットワーク、
104…ファイルサーバ、105…ファイルサーバ、
106…診療データファイル、107…保健医療カード、
201…アクセス制御設定ファイル、202…患者ID、
203…暗号化用鍵、204…相互認証用鍵、20

5…アドレステーブル、206…診療データファイル、
207…患者ID、208…アクセス制御設定情報、
209…各診療データ、301…アクセス制御設定
ファイル記憶領域、302…鍵生成モジュール、501…病
院、502…病院、503…ネットワーク、504ファ
イルサーバ、505ファイルサーバ、506診療デー
タファイル、507…患者宅端末、601…アクセス制
御設定ファイル記憶領域、602…鍵生成モジュール、

【図1】

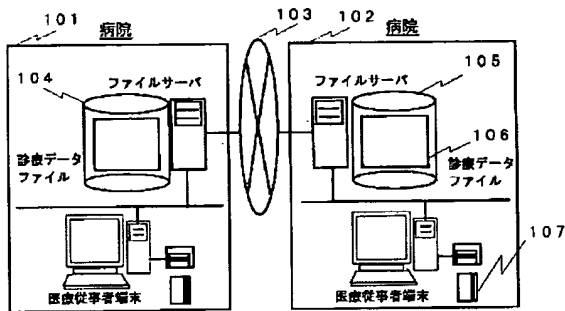


図1

【図3】

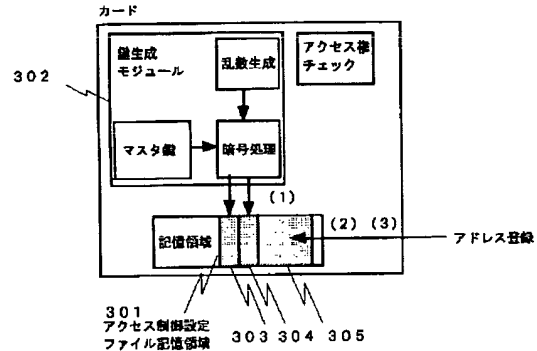


図3

【図2】

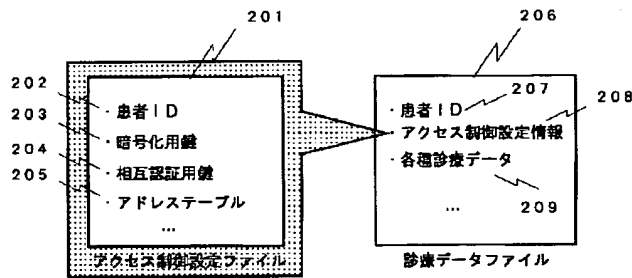


図2

【図5】

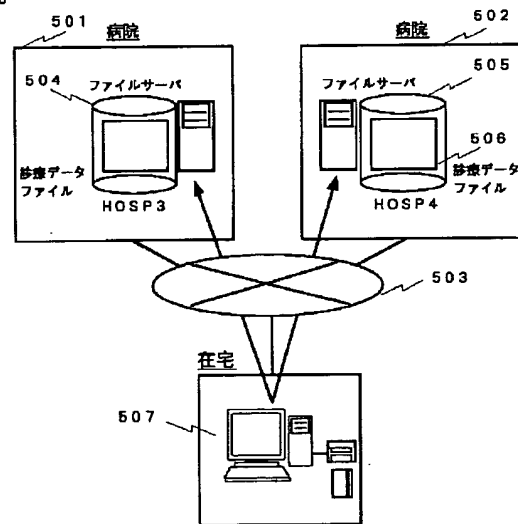


図5

【図6】

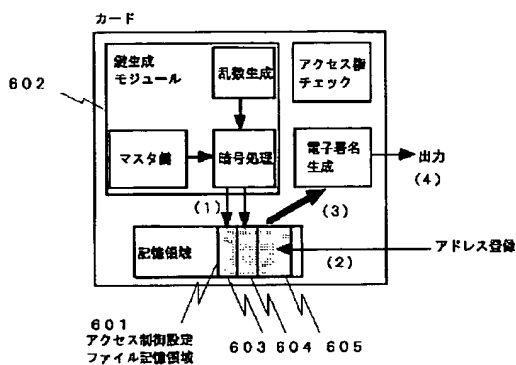


圖 6